السلام عليكم ورحمة الله وبركاتة

تعرف على فيروسات الموبايل وكيفية الحماية منها

دعونا نتعرف في البداية على فيروس الموبايل الذي نعبر عنه بكلمة (malware) اختصاراً لـ (malicious mobile software) أي البرنامج الخبيث للموبايل . وهو عبارة عن برنامج تتم برمجته على الكمبيوتر ومعد بشكل خاص للعمل في بيئة أنظمة الهواتف النقالة بهدف إحداث أضرار معينة ويتمتع فيروس الموبايل بالقدرة على الانتقال من موبايل مصاب إلى آخر وهكذا . وهناك طرق عديدة لانتقال فيروسات الموبايل ومنها :

- عبر الإرتباطات التي تأتي مع البريد الالكتروني (attachments) .
- عن طريق الملفات المتلقاه سواءاً تم تحميلها من الويب أو عن طريق وسائل الاتصال الأخرى كالـــ Bluetooth مثلاً .

وكما أن معظم هذه الفيروسات لا يبدأ تأثيرها الضار على الموبايل إلا عند تثبيتها (تفعيلها) على نظام جهاز الموبايل مع العلم أن بعض أنواع الفيروسات تفعل نفسها تلقائياً وتقوم بالعمل في البيئة المخفيه للموبايل وذلك يعتمد على مدى قوة وخطورة الفيروس .

وإن أشهر المخاطر التي تمارسها هذه الفيروسات على الأجهزة المصابة هي أن تقوم بحذف جميع البيانات الموجودة على الموبايل أو تقوم بإرسال رسائل وهمية وعشوائية إلى الأرقام المسجلة في قائمة الأسماء . ولكن بعد التطور الكبير في مجال صناعة الهواتف النقالة ومع انتشار استخدام الهواتف الذكية على مجال واسع زادت أنواع فيروسات الموبايل وكما تعددت المخاطر التي تسببها للموبايل المصاب فمنها ما يقوم بالتعديل على قائمة الأسماء من خلال التغيير في الأسماء و الأرقام المسجلة وبعضها يقوم بإجراء مكالمات تلقائية .

كما انتشر منذ حوالي سنة فيروس موبايل في اليابان وقد سبب مشاكل كبيرة من أبسطها أنه قام بعد أنتشاره وسيطرته على عدد كبير من الأجهزة النقالة بإجراء أتصال على أرقام الطوارئ بنفس الوقت مما أدى إلى حدوث حالة إرباك في الشبكات المحلية وبعض الشبكات توقفت عن العمل لمدة تزيد عن عشرين دقيقة .

وكما ظهر أيضاً فيروس خاص بالموبايلات التي تعمل على أنظمة ويندوز موبايل Windows Mobile (كمبيوترات الجيب) والمثير للجدل أن هذا الفيروس يتمتع بالقدرة على القفز من الكمبيوتر المكتبي أو المحمول إلى الهاتف اللاسلكي المحمول وذلك بمجرد شبك الموبايل إلى الكمبيوتر لاسلكيا أو سلكيا ويعد هذا الفيروس من فئة خيول طروادة وكما أطلق علية اسم : (Crossover) أي النطاط . ويعمل هذا الفيروس من خلال إدراك نظام التشغيل الموجود على الجهاز المصاب ، ثم ينتظر حتى يكتشف وصلة لجهاز محمول عبر برنامج ActiveSynch من ميكروسوفت ، وبذلك يمكنه القفز على الجهاز المحمول وبعد أن يعمل على نظام التشغيل في هذا الجهاز يقوم الفيروس بحذف كل الملفات الموجودة في مجلد My Documents وكما أنه ينشأ عدة نسخ من نفسه لأنه يقوم بنسخ نفسه كل مرة يتم فيها إعادة تشغيل النظام مما يؤدي إلى انخفاض واضح في مستوى أداء الجهاز .

ومع ازدياد قدرة مستخدمي الهواتف النقالة الذكية على تبادل الملفات فإن هذه الأخطار تزداد شيئاً فشيئاً .

ولكن هناك بعض الخطوات البسيطة التي تساعد المستخدمين على حماية أجهزتهم النقالة .

والآن تعلم حماية جهاز الموبايل الخاص بك من الفيروسات ؟

من المؤكد أن الكثير من الناس وخصوصا المتابعين لجديد التكنولوجيا يعلمون بهذه الطرق البسيطة والفعالة لحماية هواتفهم النقالة . وهذه الطرق هي كالتالي :

- يجب وضع الـ Bluetooth في جهاز الموبايل على الوضع المخفي (hidden mode) أي غير مرئي للآخرين (invisible mode) لأن هذا الإجراء يساعدك على منع الأجهزة الآخرى من أن تجد جهازك دون أن تمنحها أنت المعلومات الضرورية اللازمة للإتصال بجهازك وكما يساعدك أيضاً على حماية جهازك من البرامج الخبيثة التي تنتقل لوحدها باستخدام تقنية الـ Bluetooth . وكما يجب عليك تجنب برامج الـ Chat غير الـ Bluetooth لأنها بيئة مناسبة للإنتشار فيروسات الموبايل .
- كن حذراً قبل أن تفتح الارتباطات (attachments) التي تستلمها عن طريق الـ Bluetooth أو عن طريق رسائل الـ MMS أو البريد الالكتروني لأن هذه الارتباطات قد تحتوي برامج ضارة دون علمك بذلك . لذا فعليك قبل أن تفتح أي ارتباط أو تطبيق التأكد من أنه مرسل من قبل طرف معروف وموثوق به . وكما يجب تجنب أي ملف يرتبط به نص غير مألوف حتى لو كان مرسلاً من قبل شخص معرف لأن قد يكون جهاز هذا الشخص مصاب بنوع من الفيروسات التي تقوم بنسخ نفسها وإرسال النسخ إلى جميع الأسماء الموجودة في قائمة الأسماء عبر الشبكة كرسالة وسائط متعددة .
- لا تحمل أي محتوى أو تطبيق إلا من مصادر موثوق بها فإذا أردت تحميل برنامج او تطبيق من الانترنت قم بتحميله من الموقع الرئيسي للمنتج المراد تحميله لكي يكون خاليا من الملفات والبرامج الخبيثة .
- استخدم برنامجاً لمكافحة الفيروسات خاص بالموبايل (Mobile Anti-Virus) وهناك العديد من هذه البرامج وتأكد من توافق البرنامج مع جهازك وقم بتحديثه باستمرار .
- تأكد من لاحقة الملف المطلوب دائما فمثلا إذا كنت تتوقع استقبال ملف صوتي mp3 تأكد من وجود اللاحقة mp3 في نهاية اسم الملف المستلم وكذلك ملفات الصور وغيرها .

وهكذا نكون قد تعلمنا بعض الخطوات التي توفر لنا أماناً أكثر لأجهزتنا النقالة .

أتمنى أن تكونوا قد استفدتم من هذه المشاركة

والسلام عليكم

Syria -2008